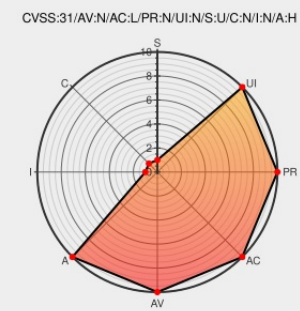
CVE-2021-46877

Published on: Not Yet Published

Last Modified on: 05/19/2023 07:11:00 PM UTC

CVE-2021-46877

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jackson-databind from Fasterxml contain the following vulnerability:

jackson-databind 2.10.x through 2.12.x before 2.12.6 and 2.13.x before 2.13.1 allows attackers to cause a denial of service (2 GB transient heap usage per read) in uncommon situations involving JsonNode JDK serialization.

CVE-2021-46877 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Possible DoS if using JDK serialization to serialize `JsonNode` · Issue #3328 · FasterXML/jackson-databind · GitHub	github.com text/html	MISC github.com/FasterXML/jackson-databind/issues/3328
Jackson 2.12.6 and 2.13.1 patch releases: one CVE fix	groups.google.com text/html	MISC groups.google.com/g/jackson-user/c/OsBsirPM_Vw

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fasterxml	Jackson-databind	All	All	All	All
Application	Fasterxml	Jackson-databind	2.13.0	-	All	All
Application	Fasterxml	Jackson-databind	2.13.0	rc1	All	All
Application	Fasterxml	Jackson-databind	2.13.0	rc2	All	All
Application	Fastxml	Jackson-databind	All	All	All	All
Application	Fastxml	Jackson-databind	2.13.0	-	All	All
Application	Fastxml	Jackson-databind	2.13.0	rc1	All	All
Application	Fastxml	Jackson-databind	2.13.0	rc2	All	All

cpe:2.3:a:fasterxml:jackson-databind:*:*:*:*:*:*:*:*:

cpe:2.3:a:fasterxml:jackson-databind:2.13.0:-:*:*:*:*:*:*:

cpe:2.3:a:fasterxml:jackson-databind:2.13.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:fasterxml:jackson-databind:2.13.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:fastxml:jackson-databind:*:*:*:*:*:*:*:*:

cpe:2.3:a:fastxml:jackson-databind:2.13.0:-:*:*:*:*:*:*:

cpe:2.3:a:fastxml:jackson-databind:2.13.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:fastxml:jackson-databind:2.13.0:rc2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-46877 : jackson-databind 2.10.x through 2.12.x before 2.12.6 and 2.13.x before 2.13.1 allows attackers to… twitter.com/i/web/status/1…	2023-03-18 22:08:22
/r/netcve	CVE-2021-46877	2023-03-18 23:38:22

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report